SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

SFC Cybersecurity Webinar

February 2025

Disclaimer and Reminder

Where this presentation refers to certain aspects of relevant requirements and expected standards on cybersecurity published by the Securities and Futures Commission (SFC), it provides information of a general nature that is *not* based on a consideration of specific circumstances. Furthermore, it is *not* intended to cover all requirements that are applicable to you or your firm. Accordingly, it should not be regarded as a substitute for seeking detailed advice on any specific case from your own professional adviser.

The SFC is the owner of the copyright and any other rights in the PowerPoint materials of this presentation. Such materials may not be reproduced for or distributed to third parties, or used for commercial purposes, without the SFC's prior written consent.

SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

(1) Overview of internet broking industry landscape in Hong Kong

(2) Cybersecurity incidents

(3) Emerging cybersecurity risk areas

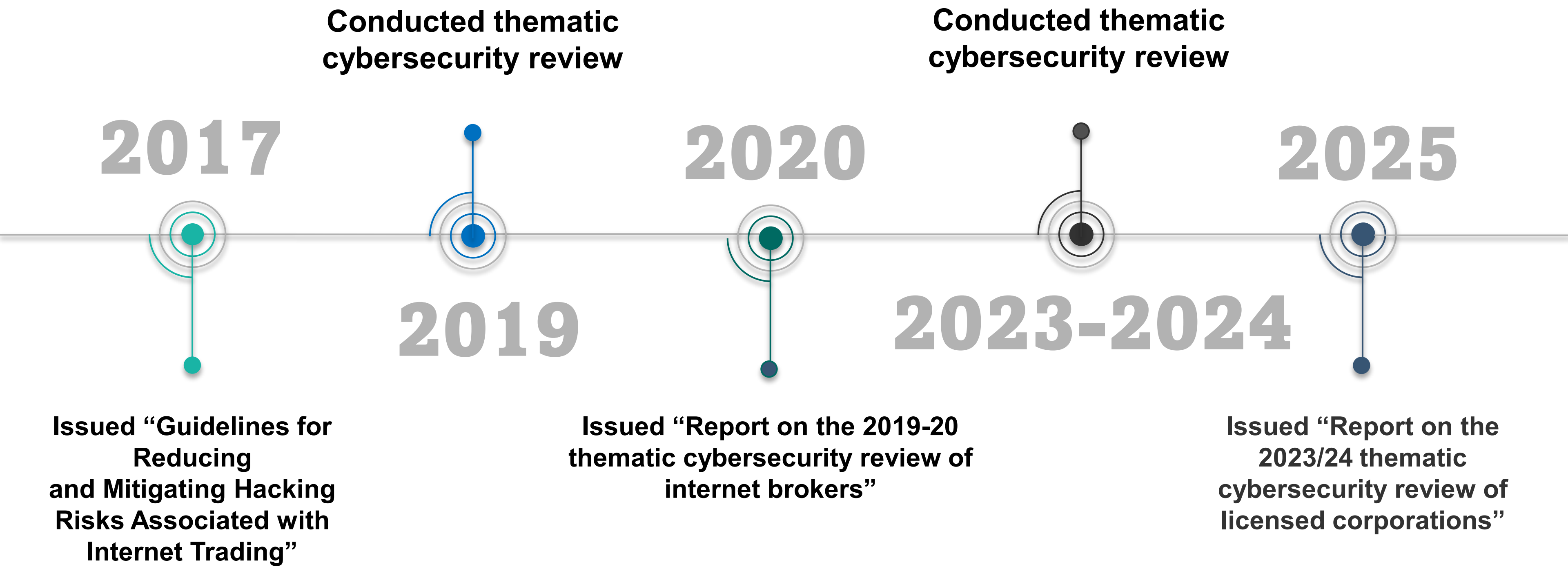
Speaker:

Steve Poon

Associate Director and Head of Suptech

Intermediaries Supervision

SFC’s key cybersecurity initiatives



2017

Issued “Guidelines for Reducing
and Mitigating Hacking Risks Associated with Internet Trading”

2019

Conducted thematic cybersecurity review

2020

Issued “Report on the 2019-20 thematic cybersecurity review of internet brokers”

2023-2024

Conducted thematic cybersecurity review

2025

Issued “Report on the 2023/24 thematic cybersecurity review of licensed corporations”

2023/24 Thematic Cybersecurity Review

50

Surveyed selected LCs of different sizes and business types, including **securities and futures brokers**, **leveraged foreign exchange trading firms**, **fund managers which provide online distribution platforms**, as well as **global financial institutions** engaged in carrying out multiple regulated activities.

Phishing

EOL software management

Cloud security

Remote access controls

Third party provider management

7

Performed on-site inspections of seven internet brokers to review their systems, procedures, and controls

6

Conducted discussions with six LCs, which had global operations, to gain insight of the cybersecurity practices adopted

Internet broking industry landscape in Hong Kong

Percentage of active clients who traded in securities, futures and leveraged foreign exchange products through internet

2021		2023
90%	→	**96.9%** ▲

BRMQ* submitted by internet brokers shows that:

92% *Implemented internet trading systems provided and supported by third-party IT service providers (third party providers)*

70% *of internet brokers used the internet trading systems provided by top* ***five*** *vendors*

30% *of the market share belonged to the largest vendor in the market*

** BRMQ refers to Business and Risk Management Questionnaire*

Internet trading channels

Clients in general prefer more flexible and accessible trading methods.

Mobile application has replaced desktop application as the most common internet trading channel offered by LCs.

	2019/20	2023/24
Desktop application	82%	31% ⌄
Mobile application	80%	80%
Trading website	65%	62% ⌄

SECURITIES AND
FUTURES COMMISSION
證券及期貨事務監察委員會

(1) Overview of internet broking industry landscape in Hong Kong

(2) Cybersecurity incidents

(3) Emerging cybersecurity risk areas

Speaker:
Markus Au Yeung
Manager
Intermediaries Supervision

Cybersecurity incidents

8

material cybersecurity incidents reported to the SFC between 2021 and 2024.

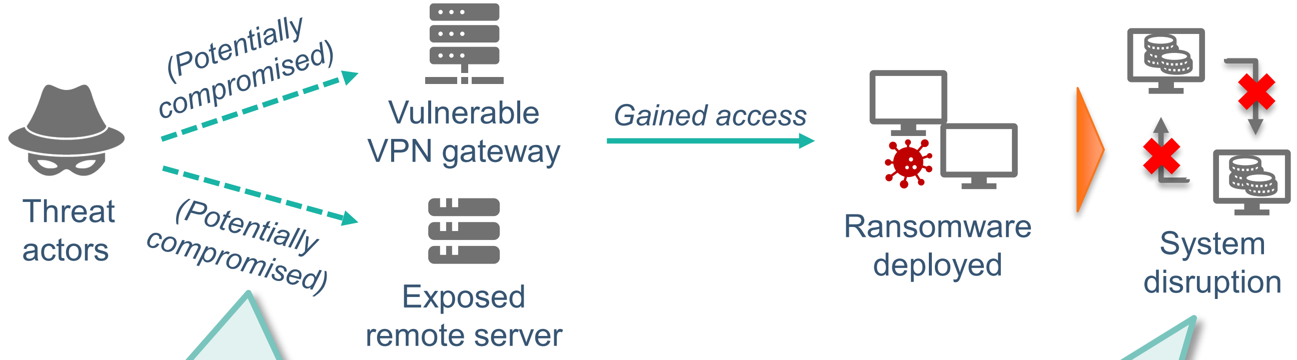
Some LCs violated most of the baseline requirements and expected standards and eventually suffered **ransomware attack**.

An LC's back-office services were disrupted when its **vendor's network was compromised.**

There were significant **security loopholes** in some LCs' networks, through which fraudsters gained access to LCs' trading systems, took over some clients' account and conducted **unauthorised transactions.**

Case illustration 1

Case example 1



⚠ Internet trading service had been suspended.

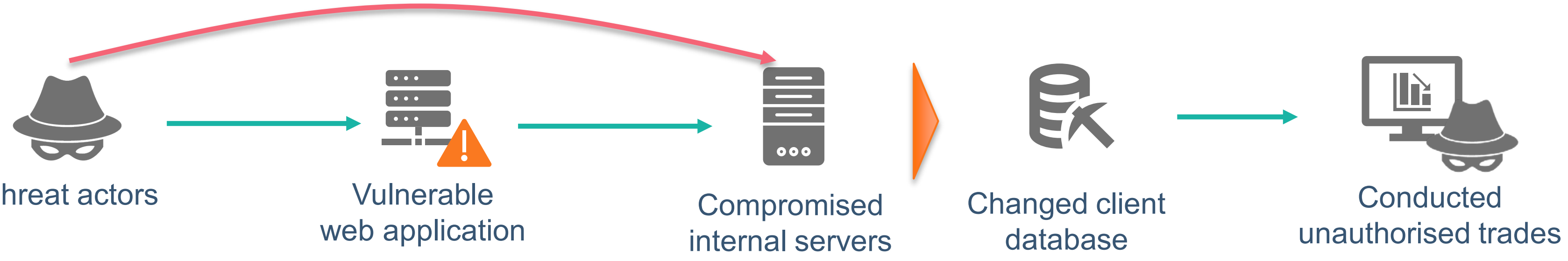
Client money deposits and withdrawals could not be processed.

☒ Due to lack of log availability, the LC could only narrow down possible root causes of the security breach.

☒ Systems, including its internet trading platform, settlement and back-office systems, were disrupted.

Case illustration 2

Case example 2



Threat actors

Vulnerable web application

Compromised internal servers

Changed client database

Conducted unauthorised trades

Web application had multiple unpatched security flaws, which had been exploited by the threat actors.

Data-in-transit and data-at-rest were not properly encrypted.

EOL software used for database.

Lesson learned

LCs should pay particular attention to the following areas:

01 Network security

02 Patch management

03 User access rights

04 Data encryption

05 Audit logs

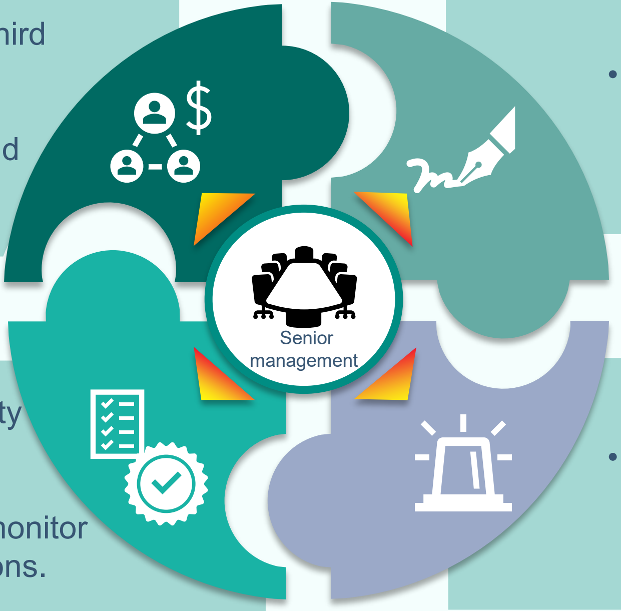
06 Monitoring of client accounts

Senior management responsibility

Senior management, in particular the MIC-IT, is ultimately responsible for the identification, monitoring and mitigation of the cybersecurity risks faced by LCs.

- Ensure that qualified staff and third party providers are appointed
- Deploy adequate technology and financial resources

- Review and approve cybersecurity risk management policies regularly



- Ensure that regular cybersecurity reviews are conducted
- Review findings, endorse and monitor the completion of remedial actions.

- Establish and maintain adequate contingency plans

SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

(1) Overview of internet broking industry landscape in Hong Kong

(2) Cybersecurity incidents

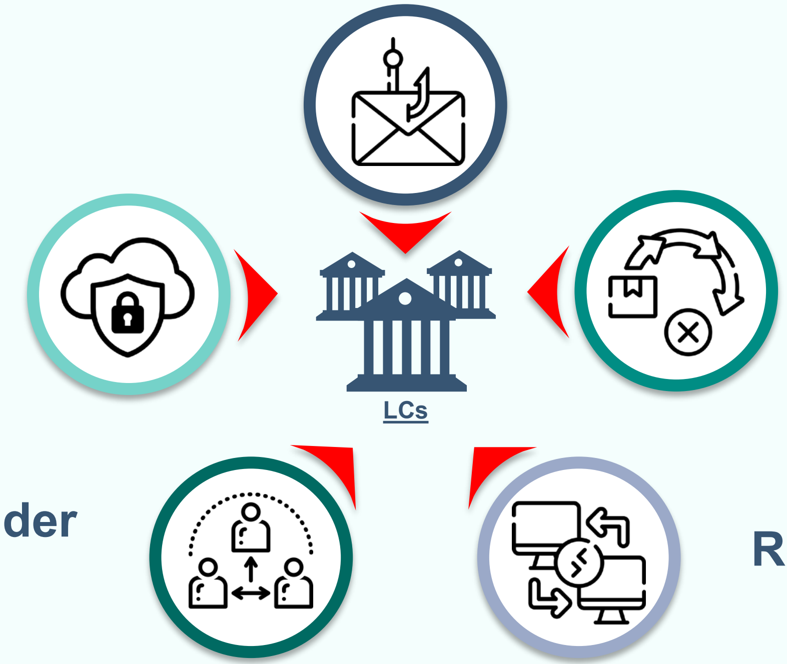
(3) Emerging cybersecurity risk areas

Speakers:

Leo Yan
Senior Manager
Intermediaries Supervision

Ada Leung
Manager
Intermediaries Supervision

Emerging cybersecurity risks



Phishing detection and prevention

Cloud security

End of life software management

Third party provider management

Remote access

Phishing detection and prevention – Expected standard

1

Deploy **anti-malware solutions** to all servers and workstations

2

Should not send electronic message with embedded hyperlinks that direct clients to LC's websites or mobile applications

3

Regular cybersecurity awareness training to staff and clients

4

Ensure cybersecurity incident handling and reporting policies and procedures cover phishing attack scenarios

Phishing detection and prevention – Examples of measures implemented by LCs

Protect the internal system and data

- Adopt email security solutions
- Add warnings to external emails

- Block access to uncategorised websites by web filtering tools
- Block phishing SMS messages

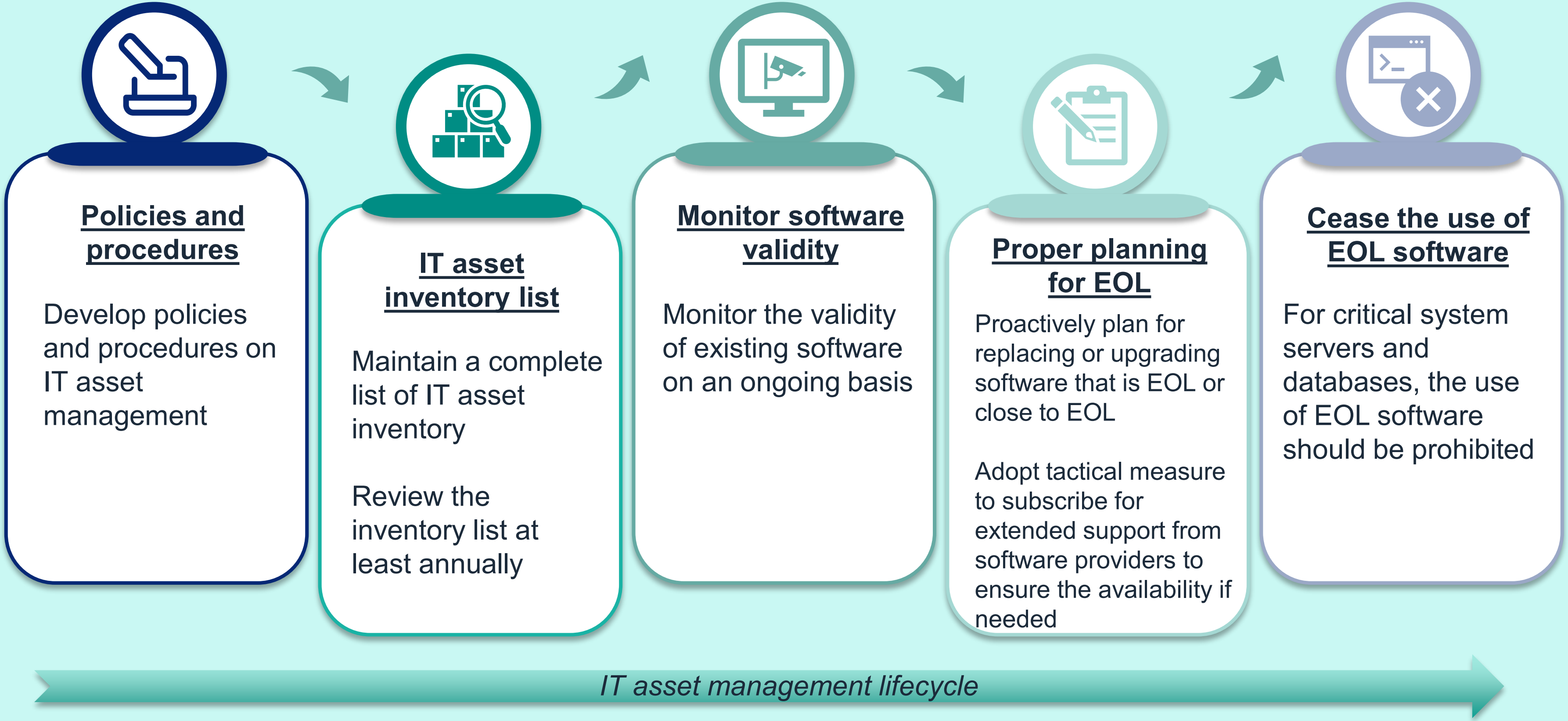
Improve staff and client awareness

Conduct regular phishing exercise

Encourage prompt reporting of phishing attempts

Participate in SMS Sender Registration Scheme

End of life software management – Expected standard



Policies and procedures

Develop policies and procedures on IT asset management

IT asset inventory list

Maintain a complete list of IT asset inventory

Review the inventory list at least annually

Monitor software validity

Monitor the validity of existing software on an ongoing basis

Proper planning for EOL

Proactively plan for replacing or upgrading software that is EOL or close to EOL

Adopt tactical measure to subscribe for extended support from software providers to ensure the availability if needed

Cease the use of EOL software

For critical system servers and databases, the use of EOL software should be prohibited

IT asset management lifecycle

End of life software management – Examples of measures implemented by LCs

Identification of software inventory

Use software or tool for IT asset management

Implement automated tool to identify software used

Planning and monitoring of EOL

Plan the EOL software replacement **24 months prior** to the date of EOL

Develop customised dashboard or risk matrix to keep track of all EOL replacement

Involve senior management in EOL remediation status discussions

Remote access – Expected standard

Policies and procedures

Develop policies and procedures on remote access management

Controls over third party providers

Avoid granting permanent access

Log and monitor activities conducted

Access rights assignment

Grant remote access rights on a “least privileged” and need-to-have” basis

Regular review

Remove unnecessary remote access rights in a timely manner, and ensure LC’s senior management review the access on regular basis (at least annually)

Security controls

Implement adequate security controls over remote access to its internal network

Remote access – Examples of measures implemented by LCs

Protect internal system and data

- Disallowed copy and paste and drive mapping features in remote access solutions
- Place remote access resources in a demilitarised zone

Prevent and identify unauthorised remote access

- Detect and block abnormal remote access behaviour
- Implement IP whitelisting control for remote connection by third party provider

Third party provider (TPP) management – Expected standard

Establish policies and procedures

Maintain a complete list of TPPs

Conduct due diligence

Ensure SLA included cybersecurity related matters

Regularly review and monitor TPP's performance

Ensure the configuration or systems supplied by TPP complies with relevant requirements

Incorporate the unavailability of TPPs into BCP

Third party provider (TPP) management – Examples of measures implemented

Selection process

- Checklist or questionnaire approach
- Conduct interview, assessment and on-site inspection (for high-risk TPPs)
- Review third-party assurance reports and certifications, ie, ISO/IEC 27001

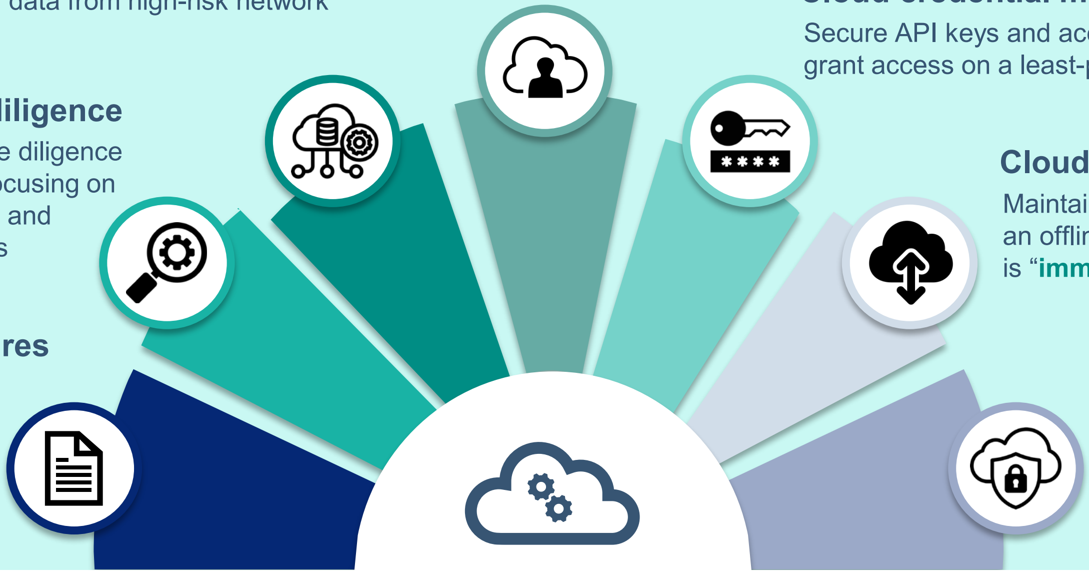
Contract management

Develop standard contract templates that outline cybersecurity measures expected of TPP

Risk management and contingency planning

- Establish appropriate arrangement to cater for service disruption or unexpected events on TPPs
- Coordinate with TPPs to perform drill tests
- Performed **post-incident analysis** to assess potential impacts with the TPPs
- Identify the **interdependencies** amongst TPPs

Cloud security – Expected standard



Policies and procedures

Develop comprehensive cloud security management covering key risk areas

Due diligence

Conduct thorough due diligence on cloud providers, focusing on their security controls and compliance measures

Cloud infrastructure security and segmentation

Implement **cloud-native segmentation** and **micro-segmentation** to isolate critical systems and data from high-risk network segments

Root account security

Enforce strict controls on cloud root account access to prevent unauthorised usage

Cloud credential management

Secure API keys and access tokens, and grant access on a least-privilege basis

Cloud backup strategy

Maintain daily backups of critical data in an offline medium; also ensure the backup is “**immutable**” and “**air-gapped**”

Contingency planning

Collaborate with third-party cloud service providers to formulate the cloud-related cybersecurity and unavailability scenarios in BCP

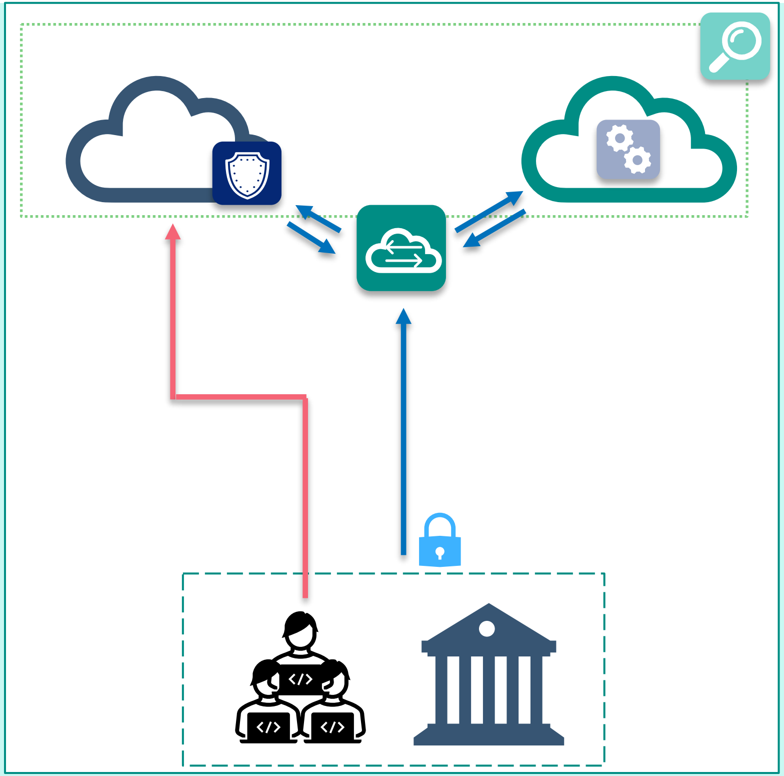
Cloud security – Examples of measures implemented by LCs

Adopt zero-trust architecture

Enforce identity and access management controls

Conduct technical security assessment

- Vulnerability scan
- Penetration test
- Configuration review



Implement advanced cloud-related security tools

- Cloud Access Security Brokers (CASB)
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platforms (CWPP)
- Cloud-Native Application Protection Platforms (CNAPP)

Use of SMS OTP for authentication

HKMA

***Enhancement measures for online payment card transactions* - 10 Oct 2024**

Mobile banking – Authentication of online payment card transactions

Customers are required to authenticate transactions via a bound device by default. For customers without mobile banking apps, they *may continue to use* SMS OTPs, while the AI should tighten their fraud monitoring on SMS OTPs authenticated activities.

MAS

Monetary Authority of Singapore

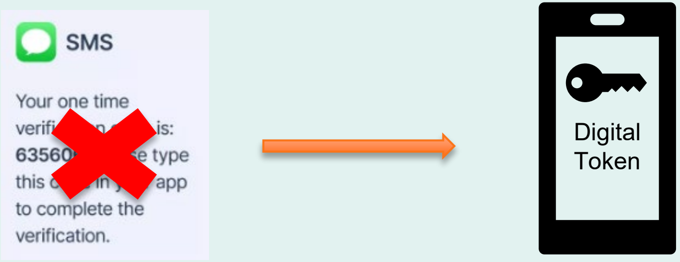
***Banks in Singapore to Strengthen Resilience Against Phishing Scams*- 9 Jul 2024**

For bank account login by customers who are digital token users

Major retail banks in Singapore will progressively phase out the use of **One-Time Passwords (OTPs),** replacing with digital token.

The digital token will authenticate customers' login without the need for an OTP that scammers can steal, or trick customers into disclosing.

In response to the security concerns associated with SMS OTP, LCs are encouraged to stop the use of SMS OTP *for authentication,* and replace it with more secure methods, such as **biometrics** and **digital token.**



SMS

Your one time verifi n is: 63560 e type this in app to complete the verification.

Way forward

To better provide guidance to all LCs in better managing cybersecurity risks:

- *Issued the 2023/24 thematic cybersecurity report on 6 February 2025*
- *Comprehensively review the existing cybersecurity requirement and expectation*
- *Develop an industry-wide cybersecurity framework*

Thank you.

www.sfc.hk